

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/768,130	01/23/2001	Yasuyuki Murakami	81942.0008	3323

26021 7590 08/23/2004
HOGAN & HARTSON L.L.P.
500 S. GRAND AVENUE
SUITE 1900
LOS ANGELES, CA 90071-2611

EXAMINER

SIMITOSKI, MICHAEL J

ART UNIT PAPER NUMBER

2134

DATE MAILED: 08/23/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/768,130

Applicant(s)

MURAKAMI, YASUYUKI

Examiner

Michael J Simitoski

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 23 January 2001.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-7 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-7 is/are rejected.
- 7) ☒ Claim(s) 3 and 5 is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 23 January 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date 1/23/01.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____.

DETAILED ACTION

1. The IDS of 1/23/2001 was received and considered.
2. Claims 1-7 are pending.

Claim Rejections - 35 USC § 101

3. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

4. Claim 7 is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The claimed subject matter relates to a signal, per se and is therefore not tangibly embodied on a computer readable medium.

Claim Objections

5. Claim 3 is objected to because of the following informalities: "second entity as a destination of ciphertext" is unnecessary. A more appropriate limitation would be "second entity, which is receiving the ciphertext". Appropriate correction is required.

Claim Rejections - 35 USC § 112

6. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

7. Claim 2 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the

invention. The limitation “generating ... using ... information obtained by dividing identification information of the first entity into a plurality of blocks and hash values” is indefinite as it is unclear if the identification information is divided into blocks *and* hash values, or whether the secret key is generated using divided information and hash values. *For the purposes of this Office Action, the secret key is understood to be obtained using divided identification information and hash values.*

Claim Rejections - 35 USC § 102

8. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

9. Claims 1-4 & 6-7 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent 5,966,449 to Iwamura et al. (Iwamura).

Regarding claim 1, Iwamura discloses dividing authentication information of an entity into a plurality of blocks (col. 9, lines 27-30 & 54-57) for each of the key generating agencies (col. 2, lines 58-65), selecting a plurality of bits of any order for each of the key generating agencies (col. 9, lines 1-5) from a predetermined sequence so as to set a hash value/g (col. 9, lines 1-9) for each of the key generating agencies and generating the secret keys/kAB of the entity by using the divided identification information/ID and the hash values/g (col. 8, lines 30-34).

Regarding claim 2, Iwamura discloses generating secret keys/ k of the first entity/A by using respective divided identification information obtained by dividing identification information of the first entity into a plurality of blocks (col. 9, lines 27-30 & 54-57) and hash values/ g_{ij} (col. 9, lines 1-9), each consisting of a plurality of bits, set for a plurality of key generating agencies (col. 2, lines 58-65), respectively, generating a common key/ k_{AB} by using components corresponding to the second entity/B (col. 8, lines 9-11), contained in the generated secret keys/ G_i (col. 9, lines 1-15) and encrypting the plaintext/ M into a ciphertext/ C by using the generated common key/ k_{AB} (col. 8, lines 19-23), wherein the hash values/ g_{ij} (col. 9, lines 1-9) are set for the key generating agencies, respectively, by selecting a plurality of bits of any order for each of the key generating agencies from a predetermined sequence of a plurality of bits (col. 9, lines 1-5).

Regarding claims 3-4 & 6-7, Iwamura discloses sending from each of a plurality of key generating agencies (col. 2, lines 58-65) to each of the first/A and second/B entities a secret key/ G_i generated by using each of divided identification information obtained by dividing identification information of each entity into a plurality of blocks (col. 9, lines 27-30 & 54-57) and a hash value/ g_{ij} (col. 9, lines 1-9) which consists of a plurality of bits and is set for each of the key generating agencies, at the first entity, generating a first common key/ k_{AB} by using components corresponding to the second entity/ IDB (col. 8, lines 19-23) as a destination of ciphertext, contained in the secret keys/ G_i of the first entity sent from the key generating agencies, respectively, at the first entity, encrypting a plaintext/ M into a ciphertext/ C by using the generated first common key/ k_{AB} and transmitting the ciphertext/ C to the second entity/B (col. 8, lines 19-23), at the second entity/B, generating a second common key/ k_{AB} identical with

Art Unit: 2134

the first common key/kAB by using components corresponding to the first entity/A, contained in the secret keys/G of the second entity sent from the key generating agencies, respectively (col. 8, lines 30-34) and at the second entity/B, decrypting the transmitted ciphertext/C into a plaintext/M by using the generated second common key/kAB, wherein the hash value/g is set for each of the key generating agencies, by selecting a plurality of bits of any order for each of the key generating agencies from a predetermined sequence of a plurality of bits (col. 2, lines 58-65).

Allowable Subject Matter

10. Claim 5 is objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael J. Simitoski whose telephone number is (703)305-8191. The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m.. The examiner can also be reached on alternate Fridays from 6:45 a.m. – 3:15 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on (703)308-4789.

Any response to this action should be mailed to:

Commissioner of Patents and Trademarks
Washington, DC 20231

Or faxed to:

(703)746-7239 (for formal communications intended for entry)

Or:

Art Unit: 2134

(703)746-7240 (for informal or draft communications, please label "PROPOSED" or "DRAFT")

Hand-delivered responses should be brought to Crystal Park II, 2121 Crystal Drive, Arlington, VA 22202, Fourth Floor (Receptionist).


Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-9000.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



MJS

August 9, 2004



GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100